REMARKS/ARGUMENTS

The foregoing amendments and the remarks that follow are intended to impart precision to the claims, and more particularly point out the invention, rather than to avoid prior art.

Claims 1-3, 10-14, 21, 23, and 24 are pending in the application. Claim 23 has been amended, and new claim 25 added above. No new matter has been added.

CLAIM REJECTIONS - 35 USC § 103

The Examiner has rejected claims 1-3, 10-14, 21 and 23-24 over Abbott et al. (U.S. Patent No. 6,671,808) (hereinafter "Abbott"), and further in view of Burger (U.S. Application Publication No. 2005/0060586 A1) (hereinafter "Burger").

Applicant's independent claim 24 recites a "secure key device comprising a storage medium configured to store . . . an encrypted log of identifiers of locations at which the secure key device has been used." The Examiner is kindly requested to note that the secure key device is recited to store the log of identifiers. This is important to keep in mind for the discussion below.

The Examiner has now gratefully recognized in the latest Office Action that Abbott does not "specifically discuss in detail . . . the identity of locations of network nodes to which apparatus communicated during transactions." Therefore, the discussion below focuses on the secondary reference Burger.

The Examiner describes that Burger discloses a list of authorized locations for interface stations 104 stored in database 406 of the network server 114 (par. 0146, Figs. 1 and 4) where the Pocket Vault can be used by sending an interface unit identifier to the network server. The Examiner concludes from this that Burger teaches accessing an authorized location by sending an identifier to a central server.

First, the Examiner is kindly requested to note that Burger states in paragraph 0146 that the "list of currently authorized or registered interface stations 104" is "stored in the database 406." Importantly, database 406 is in network server 114 (see par. 0144 and Fig. 4) and not in the Pocket Vault. Thus, Burger teaches away from storing the list of interface stations on the Pocket Vault.

To further emphasize this teaching away, in Fig. 24 Burger illustrates a transaction involving the Pocket Vault. Specifically, it is first determined that the Pocket Vault use is authorized (step 2006 in Fig. 24; par. 0512). Then, Burger describes that "information regarding the transaction is logged into the database 406 of the network server 114 (FIG. 4). As shown, the logged information may include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction." (par. 0517). Burger is teaching to store this information on network server 114. This teaches away from storing a log of identifiers on a secure key device as recited in Applicant's claim 24.

Burger describes that the Pocket Vault 102 has read/write memory 210 and write-once memory 212 (Fig. 2). Burger describes that memory 210 stores various types of media (par. 0127), but Burger does not teach or suggest memory 210 as storing a log of location identifiers. Burger describes write-once memory 212 as storing a user's fingerprints (par. 0183), but Burger also does not teach or suggest memory 212 as storing any log of location identifiers. Thus, Burger fails to teach or suggest any storage of a log of location identifiers in the Pocket Vault memory 210 or 212.

The Examiner argues that it would have been obvious to combine the teachings of Abbott and Burger because the combination would "generate a log of transactions and locations where [the] device was communicated and used." However, Burger clearly teaches away from Applicant's claim 24 because Burger teaches any such log of locations would be stored in database 406 of the network server 114 (and not the Pocket Vault) as discussed above.

Accordingly, in light of the above, Applicant respectfully submits that claim 24 is allowable.

Applicant's independent claim 1 recites that a "storage medium [of the apparatus] is configured to store . . . [a] log of unique identifiers of locations the apparatus and the individual have visited." Also, Applicant's independent claim 11 recites that "the storage medium [of the device] is configured to store . . . an encrypted log of unique identifiers of locations the apparatus and the individual have visited." Thus, Applicant's claims 1 and 11 are also respectfully believed allowable at least for the reasons discussed above for claim 24.

NEW CLAIMS

New claim 25 has been added by amendment. Claim 25 depends from claim 24 discussed above, and is believed allowable at least for the reasons discussed above.

CONCLUSION

All of Applicant's previously-pending dependent claims depend, directly or indirectly, from independent claims 1 and 11, and are believed allowable for at least the reasons discussed above. Applicant believes that the Examiner's other arguments not discussed above are moot in light of the above arguments, but reserves the right to later address these arguments.

It is respectfully submitted that all of the Examiner's objections have been addressed and that the application is now in order for allowance. Accordingly, reconsideration of the application and allowance thereof is courteously solicited.

Authorization is hereby given to charge our Deposit Account No. 50-2638 for any charges that may be due. Furthermore, if an extension is required, then Applicant hereby requests such an extension.

Respectfully submitted,

Date: May 11, 2009

Bruce T. Neel
Reg. No. 37,406

Customer Number 64494
GREENBERG TRAURIG, LLP
(650) 328-8500 Telephone
(650) 328-8508 Facsimile
wardj@gtlaw.com